УДК 004.056.5

Л.В. Константинова[1]
Кіровоградський національний технічний університет

Аналіз технології "хмарних" антивірусів

Проведені дослідження свідчать про безперервне збільшення кількості шкідливих програм. Наприклад, останній звіт "Лабораторії Касперського" відображає стрімке зростання числа нових вірусів і кількість нових загроз продовжує стрімко збільшуватися. Уже сьогодні безліч користувачів на власному досвіді переконалися, що використання хмарних технологій не просто ефективно, але є одним з найбільш перспективних напрямків для майбутнього розвитку комп'ютерної індустрії. Виходячи з цього актуальною стає задача в дослідженні технології хмарних антивірусів. Хмарні обчислення - це технологія обробки даних, в якій комп'ютерні ресурси і потужності надаються користувачеві як інтернет-сервіс. Користувач має доступ до власних даних, але не може управляти і не повинен піклуватися про інфраструктуру, операційну систему і власне про програмне забезпечення, з яким він працює.

Ідея, покладена в основу хмарних антивірусних продуктів являє собою наступне: виділяється клієнтська і серверна частини cloud-антивіруса. Перша має мінімальний розмір, встановлюється на машини користувачів і містить в своєму складі движок, який сканує дані і відправляє контрольні суми файлів на сервер. Дислокований в хмарах сервер приймає від клієнтів хеши файлів, шукає їх в базі сигнатур вірусів і видає свій вердикт щодо чистоти надісланих даних. У разі виявлення шкідливого програмного забезпечення, сервер відсилає клієнтові відповідні скрипти, виконання яких очищає користувальницький комп'ютер від шкідливих об'єктів. Подібна схема взаємодії не тільки дозволяє істотно знизити навантаження на апаратні ресурси комп'ютера, але і звільняє користувача від необхідності постійно завантажувати бази сигнатур, а також забезпечує найкращий захист за рахунок застосування системи "колективного розуму", що використовує отриману від багатомільйонної аудиторії інформацію для автоматичного виявлення і класифікації нових видів шкідливих програм.

Недоліками цієї технології є залежність від пропускної здатності мережного з'єднання і низька швидкість реакції при пересиланні великих об'єктів по мережі. Ще одним недоліком хмарних антивірусів є прагнення транслювати в інтернет інформацію, яка може містити відомості конфіденційного характеру.

Хмарні технології в тому чи іншому вигляді застосовуються в продуктах "Лабораторії Касперського", ESET, Symantec, Agnitum, F-Secure, Alwil Software та інших вендорів, але далеко не всі компанії готові повністю перевести свої рішення на нову платформу. Ще є питання, що ставлять під сумнів широке застосування хмарних технологій в корпоративній сфері, принаймні зараз.

---

[1] викладач кафедри програмного забезпечення